AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Public Storage – 4103 S. Orchard St., Tacoma, Washington, Unit #A043 and SUBJECT DEVICES 1-2

Case No. MJ18-5315

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Public Storage – 4103 S. Orchard St., Tacoma, Washington, Unit #A043 and SUBJECT DEVICES 1-2 as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2251 (a), (e)	Production of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT REESE BERG, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/19/2018

Judge's signature

City and state: TACOMA, WASHINGTON

THERESA L. FRICKE, U.S. MAGISTRATE JUDGE
Printed name and title

USAO# 2018R01430

ATTACHMENT A

Description of Property to be Searched

The SUBJECT DEVICES, more particularly described below, which are currently in the custody of Homeland Security Investigations in Tacoma, Washington:

a. Western Digital HDD 160 GB, SN: WX50A5907905 (SUBJECT DEVICE 1)

b. MicroSD Card, 64 GB (SUBJECT DEVICE 2)

The SUBJECT LOCATION is a storage unit rented by LAMAR THOMPSON at Public Storage – 4103 S. Orchard St., Tacoma, Washington (Unit # A043). The search is to include the entirety of that storage unit, as well as any digital devices found therein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found on the SUBJECT DEVICES or at the SUBJECT LOCATION:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media or other evidence of the creation of such visual depictions.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP address 73.53.83.83 (the SUBJECT IP ADDRESS) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Reese Berg, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7). I am currently employed as a Special Agent with Homeland Security Investigations (HSI). I have been a federal law enforcement officer for over 15 years. I have investigated and/or participated in investigations involving narcotics smuggling, human trafficking/smuggling, firearms trafficking, child pornography and child exploitation. I have also held positions in law enforcement as a Military Police Officer and Military Police Investigator with the U. S. Army for over 20 years. I am a graduate of the 9-week Criminal Investigator Training Program as well as the Immigration and Customs Enforcement Special Agent Training program at the Federal Law Enforcement Training Center in Glynco, Georgia. I am currently assigned as a Special Agent with HSI Seattle, where my duties include child exploitation and child pornography investigations. I have participated in more than fifty child exploitation or child pornography investigations and have worked extensively with other investigators involved in these types of investigations.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the two digital devices identified below and in Attachment A (the "SUBJECT DEVICES") that are currently in the custody of Homeland Security Investigations, and (the "SUBJECT LOCATION") also identified below and in Attachment A, for the things specified in Attachment B:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Western Digital HDD 160 GB, SN: WX50A5907905 (SUBJECT DEVICE 1)

b. MicroSD Card, 64 GB (SUBJECT DEVICE 2)

c. Public Storage – 4103 S. Orchard St., Tacoma, Washington, Unit #A043 (SUBJECT LOCATION)

3. The warrant would authorize a search of the SUBJECT LOCATION and any electronic devices located as well as the SUBJECT DEVICES and forensic examination, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

5. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found on the SUBJECT DEVICES or at the SUBJECT LOCATION.

II. DEFINITIONS

6. The following definitions apply to this Affidavit:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Internet Service Providers

a. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers.

Internet Protocol (IP) Addresses

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must be assigned an IP address so that the Internet traffic sent from, and directed to, that computer may be properly directed from its source to its destination. Most ISPs control the range of IP addresses.

IV. STATEMENT OF PROBABLE CAUSE

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

7. On or about October 27, 2018, Tacoma Police Department (TPD) Det. Faivre was assigned an investigation of potential Possession of Depictions of Minors Engaged in Sexually Explicit Conduct, documented under Tacoma Police Case Report number 1829700548. Det. Faivre reviewed the initial report taken by Police Patrol Officer (PPO) Newbold, which indicated that on October 24, 2018, PPO Newbold was dispatched to a place of business, McFarland Cascade located at 1640 Marc Avenue in the City of Tacoma. PPO Newbold was responding to a report of a cell phone that was believed to contain images of suspected depictions of minors engaged in sexually explicit conduct.

8. PPO Newbold arrived and contacted M.D., who is the current VP of Human Relations. M.D. advised that another employee, M.B., found a cell phone in a work area and while going through the phone in an attempt to identify its owner, discovered "selfie" style images of his co-worker, LAMAR THOMPSON, as well as sexually explicit images of children. M.B. gave the phone to the plant manager, J.H., who gave the phone to M.D. M.D. then called the police. PPO Newbold was unable to contact M.B., who had already left for the day.

9. PPO Newbold spoke with employees E.B., K.Y., and J.H.. Both J.H. and K.Y. stated that they did not see the photos or do anything with the phone. J.H. reported another employee gave him the phone and in turn he provided the phone to M.D. E.B. reported he found the phone in the breakroom on the morning of October 22, 2018, and the battery on the phone was dead, so he charged it to see if he could look at the phone to determine its owner. E.B. reported that once the phone was charged, he looked through the contacts list and located the contact information for another co-worker, whom he referred to as "Hassani". E.B. attempted to text "Hassani", but the text did not go through because the phone was not on a network. E.B. said that he then placed the phone on the desk of his supervisor, R.B.

10. E.B. said that on the morning of October 24, 2018, he was contacted by M.B., who had the phone and attempted to locate a "selfie" that might identify the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

phone's owner. M.B. discovered "personal photos" of his co-worker, whom he identified as LAMAR THOMPSON, and "disturbing photos involving children." E.B. took the phone from M.B., gave the phone to J.H., and reported their concerns. PPO Newbold collected the Samsung cell phone and placed it into the property and evidence locker at TPD Headquarters.

11. On November 7, 2018, Det. Faivre received a follow-up phone call from M.D. asking about the status of the case. M.D. reported his intention to dismiss THOMPSON, but he wanted to wait until the criminal investigation had been completed. Det. Faivre asked M.D. if he was able to provide any further information tying the cell phone to THOMPSON. M.D. reported seeing selfies of THOMPSON while he was "sticking his fingers into the vagina of a 6-year-old". Det. Faivre asked M.D. to confirm his observations, and M.D. stated that he "wouldn't be able to swear on it, I'm quite certain, but not 100%". M.D. reported there was another photo in which he saw the same female child being forced to perform oral sex on a person whom he believed to be THOMPSON, but that only "half of Thompson's face was in the frame of the picture". Det. Faivre asked M.D. to confirm he was certain and whether he would be able to testify to these facts before a judge. M.D. stated that he would. M.D. stated that there were other photos and videos that clearly show THOMPSON's face contained on the phone.

12. Using a law enforcement database, Det. Faivre located a criminal history for LAMAR ALLEN THOMPSON, DOB XX/XX/1982, who was convicted of Child Molestation in the First Degree in 2016 in King County Cause No. 14-1-04590-1KNT and received a Special Sex Offender Sentencing Alternative for which he served 68 months in prison and up to lifetime DOC supervision. According to records from that conviction, THOMPSON sexually abused two young girls. THOMPSON was dating seven-year-old VICTIM #1's aunt and abused her on two occasions while VICTIM #1 visited. VICTIM #1 reported that THOMPSON woke her up and flipped her onto her back before inserting his fingers inside of her "privates" and specifically described something "gushing" out of her vaginal area during the abuse that is believed to be lotion.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Seven-year-old VICTIM #2 is VICTIM #1's cousin. VICTIM #2 disclosed that THOMPSON rubbed lotion on the "lips" of her "vagina" during sleep over visits on numerous occasions. THOMPSON is currently classified as a level 2 sex offender and is on active supervision with the Department of Corrections. Pursuant to the conditions of sentence, THOMPSON was ordered to enter into sexual deviancy treatment, to have no contact with minors, and not to possess sexually explicit material.

13. On November 7, 2018, Det. Faivre was granted a Pierce County Superior Court Search Warrant by the Honorable Judge Orlando for the imaging and subsequent forensic examination of the Samsung phone seized by PPO Newbold.

14. On the evening of November 7, 2018, Det. Faivre and Det. Yglesias went to the Crossland Hotel at 8801 S. Hosmer Ave Room #329 to verify THOMPSON resided there and to determine if there were children present. THOMPSON was not home at the time, however, his wife, Nyeesha Thompson, confirmed the hotel was their current residence.

15. On November 8, 2018, TPD Det. Reda began the Cellebrite examination of the Samsung cell phone. The initial extraction information provided a mobile number of (253) 448-0887, which is the telephone number THOMPSON provided to DOC Corrections Officer Vilela at his last check-in. This phone number was also associated with THOMPSON during a Computer Aided Dispatch search. There were also multiple selfie-style photos on the phone that depict THOMPSON. Det. Faivre reviewed several of the files recovered during the examination and observed an image described as follows:

> **Image 1**: The image depicts a small black female child, who appears to be asleep. The left side of the child's face is exposed to the camera. There appears to be a section of hair that is resting above her right eye, and she is wearing a pink shirt with black writing on the upper left-hand corner. The word "The" can be seen with the second word appearing to begin with the letter S. Resting up against the child's nose and lips is a black adult male's penis. The male's forefinger of his left hand is depicted holding the penis against the child's face. The male's face is not depicted in the photograph.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

16. I have reviewed this image and concur with Det. Faivre's description. The child depicted in the photo appears to be under the age of ten.

17. Additionally, Det. Faivre located three other images of what appears to be a female child being sexually exploited. The photos are described as follows:

> **Image 2**: This image depicts a black female child lying on her back with something pink underneath her. The child is wearing white underwear that is being pulled to the side by an adult black male's left hand, exposing the child's vaginal area to the camera. The male depicted in the image is wearing a distinctive silver colored wedding band with diamonds across the center. The child does appear to have a few strands of pubic hair on the inside of the vagina, but there does not appear to be any hair present on the outside of the vagina, legs, or any other indication of follicular development. No other part of the child is depicted.
>
> **Image 3:** This image depicts the vaginal area of a black female child, who is lying on top of a piece of fabric that is pink with black stripes. The camera is focused on the child's vagina, which is being spread open by what appears to be the fore and middle finger of an adult black male. The male's fingernails are long and have a dark substance underneath them. The female in this photograph has slight pubic hair on the outside of the vagina, but the rest of her genital area appears to be pre-pubescent.
>
> **Image 4**: This image depicts an apparent black minor female wearing a red shirt. The shirt is being pulled up to expose the bare chest of the minor. The shirt is being held up by a black male, wearing the same wedding ring as described above. The exposed chest area reveals a small brown nipple that appears to be the left breast of the female. The breast area looks under developed, and the areola is small.

18. I have reviewed the above-described images and agree with Det. Faivre's descriptions.

19. Metadata associated with Images 1-4 show that they were taken with an Apple iPhone 7 on May 27, 2018, between 12:09 and 12:15 a.m. Associated GPS coordinates show they were created in the vicinity of an address in Tacoma, Washington. At this time, the location of the iPhone 7 responsible for producing the sexual exploitation images of the minor black female child(ren) depicted in the images described above remains unknown.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

20. On November 8, 2018, Det. Faivre contacted Washington Department of Corrections (DOC) Officer VILELA concerning THOMPSON's violations of conditions of sentence and evidence of violations of RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct and RCW 9.68A.040 Sexual Exploitation of a Minor and to seek assistance in identifying minors to whom THOMPSON may have access. Shortly thereafter, DOC Officer VILEA advised that DOC planned to arrest THOMPSON that afternoon for violation of his sentence.

21. Later that day, DOC Officer VILELA provided a photo of THOMPSON's left ring finger in depicting a ring matching the ring observed in two of the three photos depicting sexual exploitation of a minor described above. DOC Officer VILELA collected the ring as evidence and advised Det. Faivre that THOMPSON had another cell phone on his person at the time of arrest, which was taken into evidence. THOMPSON was booked into the King County Jail pending violations of sentence.

22. Because three of the above-mentioned images depicted early stages of development, Det. Faivre consulted with Dr. Elizabeth Woods at the Child Abuse Intervention Department (CAID) with MultiCare to assist in determining age on the female depicted. Det. Faivre provided several of the above-described images to Dr. Woods, who determined the depicted females lacked sexual maturation. Dr. Woods further explained that in the vaginal area, although there was a presence of pubic hair, what was lacking was an obvious "estroginated" darkening in the tissue in the vaginal area that is normally present in post pubescent females and a lack of follicular development present. Dr. Woods estimated the depicted female child(ren) were approximately 12-14 years old, and noted the estimation "generous," stating that it was entirely possible that if she were able to see more of the child, that she could be younger. Dr. Woods reviewed the image of the exposed breast and noted beginning signs of tissue development and definition, the nipple area of the breast appeared to be smaller, and that it did not appear to be raised at all from the tissue. Dr. Woods provided the same age approximation of 12-14, based on what was visible from the pictures.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

23. Det. Faivre then followed up with THOMPSON's former employer and original reporting party at McFarland Cascade regarding the address that he provided for THOMPSON in the original police report. The address given was SUBJECT ADDRESS[1] in Tacoma. M.D. confirmed that this was the address that THOMPSON provided to him during new employee orientation around May or June of this year.

24. Det. Faivre used a law enforcement database to run the address of SUBJECT ADDRESS in Tacoma to see who was listed as the current resident. Det. Faivre was provided with a name of H.S., and also noted that the same law enforcement database showed that address as being THOMPSON's from March 2018 until September 2018. As noted above, the metadata recovered from Images 1-4 show they were all created within a six-minute window on May 27, 2018, with the same model Apple iPhone and had geolocation data suggesting they were created near SUBJECT ADDRESS in Tacoma.

25. Det. Faivre conducted a Global History search on H.S. and located a Tacoma Police report from September 12, 2018, documenting an incident report where H.S.'s minor daughter disclosed to a hospital CPS worker that she had been "consistently" molested by a family friend, who was referred to only as "uncle" from the time she was four until she was fourteen. Notably, THOMPSON was referred to as "uncle" by VICTIM #1 from his 2014 Child Molestation conviction.

26. TPD Det. Josh McKenzie made numerous attempts to contact the 2018 victim through her parents and was advised that she did not wish to cooperate with an investigation or submit to a forensic interview. The case was then cleared as unfounded.

27. On November 15, 2018, Det. Faivre obtained search warrants from King County Superior Court for THOMPSON's cell phone that was on his person at the time of his arrest, his residence at the Crossland Hotel, his person, and his Google accounts.

[1] I am aware of the exact address referenced herein and referred to throughout as "SUBJECT ADDRESS in Tacoma." The specific street name and number will not be used to protect the privacy of minor(s).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

28. On November 14, 2018, Det. Faivre and Det. Yglesias went to SUBJECT ADDRESS in Tacoma and met with H.S. and his two minor daughters, L.S. and MV1. Det. Faivre immediately recognized MV1 as the child in Image 1. H.S. was shown the above photo, which had been sanitized, to see if he could identify the child. He thought it looked like MV1 but was not absolutely sure. He then called his older daughter, L.S., to examine the image, and she immediately recognized the child as MV1.

29. L.S. identified the child in the above image as her younger sister, MV1, an eight-year-old female and H.S.'s daughter. L.S. also recognized the shirt MV1 was wearing in the photo and brought the detectives to the bedroom she shares with MV1 and retrieved it from the laundry bin.

30. While Det. Faivre was in the bedroom, she noticed that the bedding on one of the beds, including a pillow case and body pillow, were of the same patterns as those visible in the images described above recovered from THOMPSON's phone.

31. Asked if THOMPSON ever lived at the SUBJECT ADDRESS in Tacoma, H.S. said he did not but stated that he visited frequently. H.S. also said that he did not believe THOMPSON ever stayed overnight.

32. On November 15, 2018, Det. Faivre, Det. Yglesias, and I went back to SUBJECT ADDRESS in Tacoma and met with K.W, MV1's mother. She was shown a sanitized version of the first described image. She immediately began to cry and said "yes, that's my baby," referring to MV1. Asked if THOMPSON had resided at SUBJECT ADDRESS in Tacoma, K.W. stated she did not believe he had lived there but said he did come to visit. K.W. noted that over the preceding months, she was in and out of the hospital and therefore could not say whether THOMPSON had ever stayed the night between May and September 2018.

33. On November 21, 2018, I went to the King County Jail and took photos of THOMPSON's hands, pursuant to the King County Superior Search Warrant.

34. On November 23, 2018, I reviewed the adult hand in Image 2 and compared it to the known photos that I had taken of THOMPSON's hands and identified

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

several similarities. I noticed that in the known photo, THOMPSON has a dark spot on the right side of his left index finger near the first knuckle. This spot is also visible in the same location on the index finger in Image 2. Further, the lines in the second knuckle of the left middle finger in the known photo appear to match the lines in the second knuckle of the left middle finger in Image 2.

35. I compared the adult hand in Image 3 photograph described above and noticed that what appears to be the left index finger in the photo has the same dark spot in the same location as the left index finger in the known photo of THOMPSON's left hand.

36. As part of my investigation I obtained recorded jail calls made by THOMPSON to his wife, Nyeesha Thompson. I have listened to several of those recordings and summarize relevant information contained in two of them below (Note that these calls were made from another inmate's account, but the parties speaking are THPMSON and his wife.)

> **11/15/18 @ 18:23:19**: THOMPSON's wife explains to him that the detectives searched their hotel room with a search warrant. THOMPSON asks if they found anything, and she says, "old phones and a laptop". THOMSPON responds, "I am cooked!" THOMPSON then asks his wife to read what the police seized from the warrant inventory, and she reads off the items taken during the search warrant. As she lists various digital devices, THOMPSTON replies, "oh, yea, they got me!" She continues and he interjects, "oh, yea. They got me. They got it all. I got stuff on there… to be honest with you right now, I got stuff on there." THOMPSON then responds to a question from his wife with, "oh, yea! When I say I'm cooked, I'm like a roasted duck!" Later in the conversation, THOMPSON says, "Those flash drives are enough to put me away forever."

> **11/15/18 @ 20:16:29**: During the call, THMPSON says, "Look, there's a lot more that you're going to find out, and I'd rather it come from me before you find out. I have done things for years. Those hard drives … it is not going to be pretty when it comes out. There's probably over 150 different things on there." Later in the call, THOMPSON says, "That stuff is really, mostly old, nothing is new. But the fact of the matter is that I still had it."

37. On November 20, 2018, Det. Faivre and I conducted a recorded interview of Nyeesha Thompson. During the interview, Nyeesha Thompson provided me with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

three blue thumb drives that were missed by investigators during the search of her and THOMPSON's hotel room on November 15, 2018. Nyeesha Thompson said the thumb drives were located in the side pocket of a blue duffel bag that belonged to THOMPSON. She said the thumb drives belong THOMPSON. I booked the thumb drives in to evidence at the HSI office in Tacoma, WA.

38. During the same interview, Nyeesha Thompson said she had previously pawned a laptop computer that belonged to THOMPSON. On November 21, 2018, Det. Faivre recovered the laptop she pawned from Cash America Pawn in Tacoma, WA, and I took custody of the laptop on November 27, 2018, and booked it in to evidence at the HSI office in Tacoma, WA.

39. A subsequent search warrant was requested and granted to search the three thumb drives and laptop.

40. On December 6, 2018, Det. Faivre and I met with a juvenile witness (JW1), for an interview. JW1 handed me SUBJECT DEVICES 1-2, unserved copies of a Petition for Order for Protection and Temporary Order for Protection and Notice of Hearing listing Nyeesha Thompson as the Petitioner and LAMAR THOMPSON as the respondent, and a hand-written letter from LAMAR THOMPSON to Nyeesha Thompson. JW1 said her father, H.S., received the items from Nyeesha Thompson and told her to give them to me. I later verified this information with H.S. and Nyeesha Thompson. After the interview, I booked SUBJECT DEVICES 1-2 in to evidence at the HSI office in Tacoma, WA.

41. Nyeesha Thompson told me she found SUBJECT DEVICES 1-2 in her hotel room as she has been cleaning up preparing to move out of the hotel. She said SUBJECT DEVICES 1-2 belonged to THOMPSON. She said the letter was sent to her by THOMPSON while he was incarcerated in the King County Jail.

42. Nyeesha Thompson also said that she obtained the Petition for Order for Protection and Temporary Order for Protection and Notice of Hearing, but it had not been served on THOMPSON. SA Acala served the orders on THOMPSON on December 13,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2018, and filed the return of service with the Pierce County Clerk's Office. That same day, THOMPSON made his initial appearance in Tacoma on a federal criminal complaint charging him with production of child pornography in violation of 18 U.S.C. § 2251(a) in Cause No. MJ18-5270..

43. Nyeesha Thompson told me that LAMAR THOMPSON has a storage unit with Public Storage. She did not know the address but said the unit number was A043. Nyeesha Thompson said that she has some furniture and clothing items in the storage unit, but most of the contents belong to LAMAR THOMPSON, including documents, computers, and other electronic devices. Nyeesha Thompson said she does not have access to the unit, and it is scheduled for public auction on December 20, 2018, due to nonpayment of the rent.

44. On December 17, 2018, I served an HSI Summons on Public Storage requesting information on any units rented by LAMAR THOMPSON. Management confirmed that Unit #A043 at 4103 S. Orchard St., Tacoma, WA, SUBJECT LOCATION, was rented by THOMPSON.

VI. TECHNICAL BACKGROUND

45. Based on my training and experience and information provided to me by computer forensic agents, I know that data can quickly and easily be transferred from one digital device to another digital device. Data can be transferred from computers or other digital devices to internal and/or external hard drives, tablets, mobile phones, and other mobile devices via a USB cable or other wired connection. Data can also be transferred between computers and digital devices by copying data to small, portable data storage devices including USB (often referred to as "thumb") drives, memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

46. As outlined above, residential Internet users can simultaneously access the Internet in their homes with multiple digital devices. Also explained above is how data can quickly and easily be transferred from one digital device to another through the use of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices (USB drives, memory cards, optical discs). Therefore, a user could access the Internet using their assigned public IP address, receive, transfer or download data, and then transfer that data to other digital devices which may or may not have been connected to the Internet during the date and time of the specified transaction.

47. Based on my training and experience, I have learned that the computer's ability to store images and videos in digital form makes the computer itself an ideal repository for child pornography. The size of hard drives used in computers (and other digital devices) has grown tremendously within the last several years. Hard drives with the capacity of four (4) terabytes (TB) are not uncommon. These drives can store thousands of images and videos at very high resolution.

48. Based on my training and experience, collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by companies such as Google, Yahoo, Apple, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

49. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

whether a computer contains wireless software, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

50. Based on my training and experience, I have learned that producers of child pornography can produce image and video digital files from the average digital camera, mobile phone, or tablet. These files can then be transferred from the mobile device to a computer or other digital device, using the various methods described above. The digital files can then be stored, manipulated, transferred, or printed directly from a computer or other digital device. Digital files can also be edited in ways similar to those by which a photograph may be altered; they can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the child pornographer in that this method of production is a difficult trail for law enforcement to follow.

51. As part of my training and experience, I have become familiar with the structure of the Internet, and I know that connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

52. Based on my training and experience, I know that cellular mobile phones (often referred to as "smart phones") have the capability to access the Internet and store information, such as images and videos. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily connect the device to a computer or other digital device, via a USB or similar cable, and transfer data files from one digital device to another.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

53. As set forth herein and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be found on the SUBJECT DEVICES and in the SUBJECT LOCATION in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

54. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly. They also may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an Internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

55. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

56. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that LAMAR THOMPSON likely has a sexualized interest in children and depictions of children. I therefore believe that evidence of child pornography is likely to be found on the SUBJECT DEVICES and at the SUBJECT LOCATION.

57. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another.

58. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

59. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. HSI agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To affect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

VII. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

60. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

as scanning areas of the disk not allocated to listed files or peruse every file briefly to determine whether it falls within the scope of the warrant.

61. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the SUBJECT DEVICES or any digital devices found at th eSUBJECT LOCATION and will specifically authorize a review of the media or information consistent with the warrant.

62. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICES and digital devices found at the SUBJECT LOCATION pursuant to this warrant as follows:

63. Securing the Data: In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICES or any digital devices located in the SUBJECT LOCATION. Law enforcement will only create an image of data physically present on or within the device. Creating an image of the digital device will not result in access to any data physically located elsewhere. However, devices that have previously connected to devices at other locations may contain data from those other locations.

64. Searching the Forensic Images: Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

VIII. CONCLUSION

65. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located on/in the SUBJECT DEVICES and the SUBJECT LOCATION as more fully described in Attachment A to this Affidavit, I therefore request that the court issue a warrant authorizing a search of the SUBJECT DEVICES and the SUBJECT LOCATION specified in Attachment A for the items more fully described in Attachment B.

Reese Berg, Affiant
Special Agent
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED and SWORN to before me this 19th day of December, 2018.

THERESA L. FRICKE
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Description of Property to be Searched

The SUBJECT DEVICES, more particularly described below, which are currently in the custody of Homeland Security Investigations in Tacoma, Washington:

a. Western Digital HDD 160 GB, SN: WX50A5907905 (SUBJECT DEVICE 1)

b. MicroSD Card, 64 GB (SUBJECT DEVICE 2)

The SUBJECT LOCATION is a storage unit rented by LAMAR THOMPSON at Public Storage – 4103 S. Orchard St., Tacoma, Washington (Unit # A043). The search is to include the entirety of that storage unit, as well as any digital devices found therein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found on the SUBJECT DEVICES or at the SUBJECT LOCATION:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media or other evidence of the creation of such visual depictions.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP address 73.53.83.83 (the SUBJECT IP ADDRESS) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970